

GRI 418: Quyền Riêng tư của Khách hàng 2016

NGÀY HIỆU LỰC: NGÀY 1 THÁNG 7 NĂM 2018

TIÊU CHUẨN THEO CHỦ ĐỀ

418

GRI 418: Quyền Riêng tư của Khách hàng 2016

Tiêu chuẩn theo Chủ đề

Ngày Hiệu Lực

Tiêu chuẩn này có hiệu lực đối với báo cáo hoặc tài liệu khác được phát hành vào hoặc sau ngày 1 tháng 7 năm 2018.

Trách nhiệm

Tiêu chuẩn này được [Hội đồng Tiêu chuẩn Phát triển Bền vững Toàn cầu \(GSSB\)](#) ban hành. Vui lòng gửi mọi ý kiến phản hồi về Bộ Tiêu chuẩn GRI tới gssbsecretariat@globalreporting.org để GSSB xem xét.

Quy trình Hợp lệ

Tiêu chuẩn này được xây dựng vì lợi ích cộng đồng và phù hợp với các yêu cầu trong Quy trình Hợp lệ của GSSB. Tài liệu này được xây dựng dựa trên chuyên môn của nhiều bên liên quan, có tham khảo các văn kiện liên chính phủ có thẩm quyền và kỳ vọng phổ biến của các tổ chức về trách nhiệm xã hội, môi trường và kinh tế.

Trách Nhiệm Pháp Lý

Tài liệu này nhằm mục đích hỗ trợ việc báo cáo phát triển bền vững và đã được Hội đồng Tiêu chuẩn Phát triển Bền vững Toàn cầu (GSSB) xây dựng thông qua quy trình tham vấn đa bên độc đáo với sự tham gia của đại diện từ các tổ chức và người dùng thông tin báo cáo trên toàn thế giới. Trong khi Hội đồng Giám sát GRI, Ban Quản lý và GSSB khuyến khích mọi tổ chức sử dụng Bộ tiêu chuẩn Báo cáo Phát triển Bền vững GRI (Bộ Tiêu chuẩn GRI) và các Diễn giải có liên quan, thì việc chuẩn bị và công bố các báo cáo dựa hoàn toàn hoặc một phần vào Bộ Tiêu chuẩn GRI và các Diễn giải có liên quan hoàn toàn là trách nhiệm của người lập báo cáo. Hội đồng Giám sát GRI, Ban Quản lý, GSSB và tổ chức Sáng kiến Báo cáo Toàn cầu (GRI) Stichting không chịu trách nhiệm về bất kỳ hậu quả hoặc thiệt hại nào phát sinh trực tiếp hoặc gián tiếp từ việc sử dụng Bộ Tiêu chuẩn GRI và các Diễn giải có liên quan trong quá trình lập báo cáo hoặc việc sử dụng báo cáo dựa vào Bộ Tiêu chuẩn GRI và các Diễn giải có liên quan.

Thông báo về bản quyền và nhãn hiệu

Tài liệu này được tổ chức Sáng kiến Báo cáo Toàn cầu (GRI) Stichting bảo vệ bản quyền. Được phép sao chép và phân phối tài liệu này để cung cấp thông tin và/hoặc sử dụng trong quá trình lập báo cáo phát triển bền vững mà không cần GRI cho phép trước khi thực hiện. Tuy nhiên, không được phép sao chép, lưu trữ, dịch hoặc chuyển giao tài liệu này hoặc bất kỳ trích đoạn nào từ tài liệu này dưới bất kỳ hình thức hoặc phương tiện nào (điện tử, cơ học, photocopy, ghi âm hoặc cách khác) cho bất kỳ mục đích nào khác nếu không có văn bản cho phép của GRI trước khi thực hiện.

Tổ chức Sáng kiến Báo cáo Toàn cầu, GRI và logo, GSSB và logo, cũng như Bộ tiêu chuẩn Báo cáo Phát triển Bền vững GRI (Bộ Tiêu chuẩn GRI) và logo là các nhãn hiệu của tổ chức Sáng kiến Báo cáo Toàn cầu (GRI) Stichting.

© 2026 GRI. Bảo lưu mọi quyền.

ISBN 978-90-8866-129-7

Mục lục

Giới thiệu	4
1. Công bố thông tin quản lý chủ đề	7
2. Công bố thông tin theo chủ đề	8
Công bố thông tin 418-1 Khiếu nại có căn cứ liên quan đến vi phạm quyền riêng tư của khách hàng và mất dữ liệu khách hàng	8
Thuật ngữ	9
Tài liệu tham khảo	11

Giới thiệu

GRI 418: Quyền Riêng tư của Khách hàng 2016 bao gồm các công bố thông tin để các tổ chức báo cáo về các tác động liên quan đến quyền riêng tư của khách hàng và cách quản lý những tác động này.

Tiêu chuẩn có cấu trúc như sau:

- **Phần 1** bao gồm yêu cầu cung cấp thông tin về cách tổ chức quản lý các tác động liên quan đến quyền riêng tư của khách hàng của mình.
- **Phần 2** bao gồm một công bố, cung cấp thông tin về các tác động liên quan đến quyền riêng tư của khách hàng của tổ chức.
- **Bảng thuật ngữ** bao gồm các thuật ngữ được định nghĩa với ý nghĩa cụ thể khi sử dụng trong Bộ Tiêu chuẩn GRI. Các thuật ngữ được gạch chân trong văn bản Bộ Tiêu chuẩn GRI và được liên kết đến định nghĩa
- **Tài liệu tham khảo** kê các văn kiện liên chính phủ có giá trị tham chiếu cao được sử dụng trong quá trình xây dựng Tiêu chuẩn này.

Nội dung còn lại của phần Giới thiệu trình bày bối cảnh của chủ đề, tổng quan về hệ thống Bộ Tiêu chuẩn GRI và thông tin bổ sung về cách sử dụng Tiêu chuẩn này.

Bối cảnh của chủ đề

Tiêu chuẩn này đề cập đến chủ đề quyền riêng tư của khách hàng, bao gồm cả trường hợp mất dữ liệu khách hàng và vi phạm quyền riêng tư của khách hàng.

Những sự cố này có thể là do không tuân thủ luật pháp, quy định hiện hành và/hoặc các tiêu chuẩn tự nguyện khác liên quan đến việc bảo vệ quyền riêng tư của khách hàng.

Những khái niệm này được nêu trong các văn kiện chính của Tổ chức Hợp tác và Phát triển Kinh tế xem phần [Tài liệu tham khảo](#).

Hệ thống của Bộ Tiêu chuẩn GRI

Tiêu chuẩn này là một phần của Bộ tiêu chuẩn Báo cáo Phát triển Bền vững GRI (Bộ Tiêu chuẩn GRI). Bộ Tiêu chuẩn GRI hướng dẫn tổ chức báo cáo thông tin về các tác động đáng kể nhất của tổ chức đối với nền kinh tế, môi trường và con người, bao gồm cả tác động đến quyền con người cũng như cách tổ chức quản lý những tác động này.

Bộ tiêu chuẩn GRI có cấu trúc như một hệ thống các tiêu chuẩn tương quan với nhau, được sắp xếp thành ba phần: Tiêu chuẩn GRI Tổng thể, Tiêu chuẩn GRI theo Ngành và Tiêu chuẩn GRI theo Chủ đề (xem [Hình 1](#) trong Tiêu chuẩn này).

Tiêu chuẩn Tổng thể: **GRI 1, GRI 2 và GRI 3**

GRI 1: Tiêu chuẩn cơ sở 2021 nêu rõ các yêu cầu mà tổ chức phải tuân thủ để báo cáo theo Bộ Tiêu chuẩn GRI. Tổ chức bắt đầu sử dụng Bộ Tiêu chuẩn GRI bằng cách tham khảo **GRI 1**.

GRI 2: Công bố thông tin Chung 2021 bao gồm các công bố thông tin mà tổ chức sử dụng để cung cấp thông tin về hoạt động báo cáo và các thông tin chi tiết khác của tổ chức, chẳng hạn như về hoạt động vận hành, công tác quản trị và các chính sách.

GRI 3: Chủ đề Trọng yếu 2021 đưa ra hướng dẫn về cách xác định các chủ đề trọng yếu. Trong đó bao gồm cả các công bố thông tin mà tổ chức sử dụng để báo cáo thông tin về quy trình xác định các chủ đề trọng yếu, danh sách các chủ đề trọng yếu và cách tổ chức quản lý từng chủ đề.

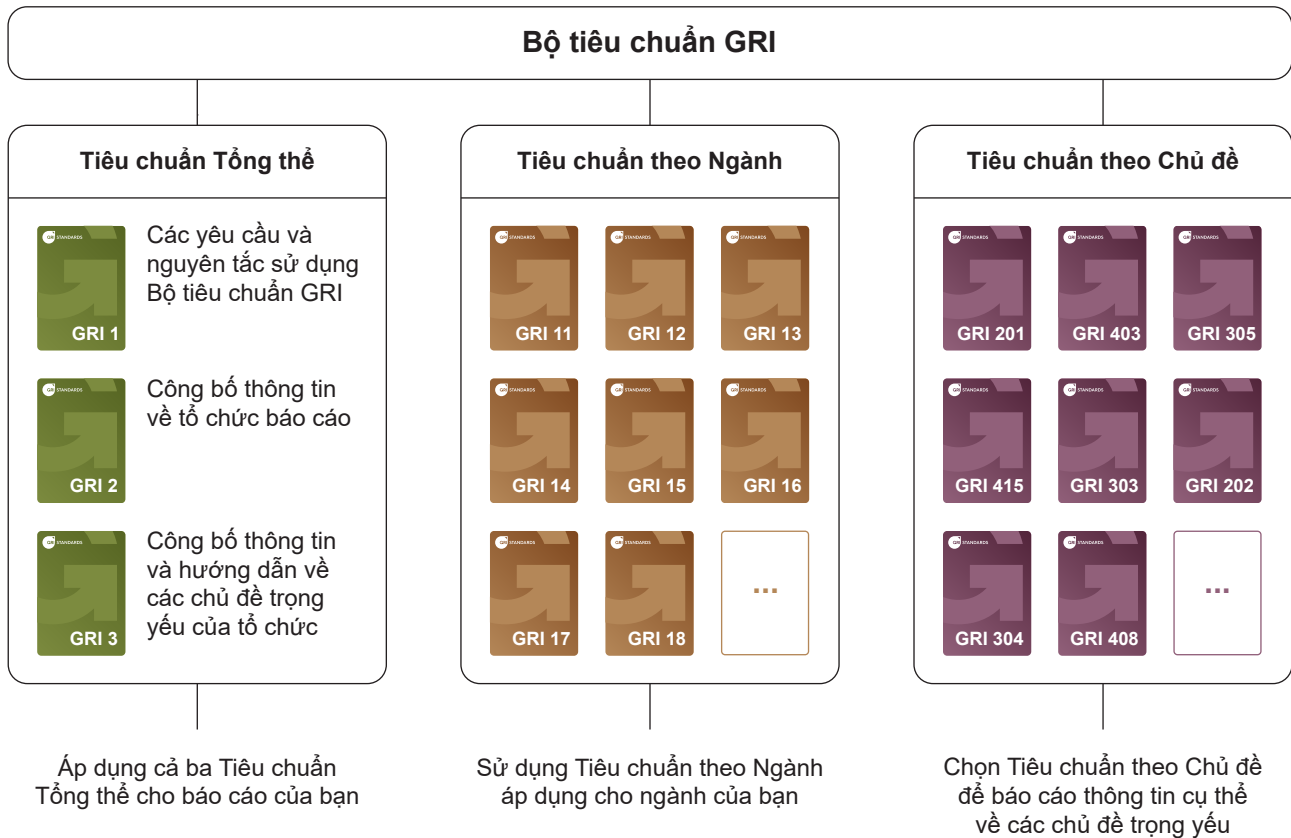
Tiêu chuẩn theo Ngành

Tiêu chuẩn theo Ngành cung cấp các thông tin cho tổ chức về những chủ đề có khả năng là trọng yếu đối với họ. Tổ chức sử dụng Tiêu chuẩn theo Ngành áp dụng cho các lĩnh vực của mình khi xác định các chủ đề trọng yếu và khi xác định nội dung báo cáo cho từng chủ đề trọng yếu.

Tiêu chuẩn theo Chủ đề

Tiêu chuẩn theo Chủ đề bao gồm các công bố thông tin mà tổ chức sử dụng để báo cáo thông tin về các tác động của mình liên quan đến các chủ đề cụ thể. Tổ chức sử dụng Tiêu chuẩn theo Chủ đề theo danh sách các chủ đề trọng yếu đã xác định thông qua *GRI 3*.

Hình 1. Bộ tiêu chuẩn GRI: Tiêu chuẩn Tổng thể, Tiêu chuẩn theo Ngành và Tiêu chuẩn theo Chủ đề



Sử dụng Tiêu chuẩn này

Tiêu chuẩn này có thể được sử dụng bởi bất kỳ tổ chức nào – bất kể quy mô, loại hình, ngành nghề, vị trí địa lý hoặc kinh nghiệm báo cáo – để công bố thông tin về các tác động liên quan đến quyền riêng tư của khách hàng của tổ chức đó.

Tổ chức báo cáo theo Bộ Tiêu chuẩn GRI phải báo cáo các công bố thông tin sau nếu đã xác định quyền riêng tư của khách hàng là một chủ đề trọng yếu:

- **Công bố thông tin 3-3 trong GRI 3: Chủ đề Trọng yếu 2021** (xem điều khoản 1.1 trong Tiêu chuẩn này);
- Bất kỳ công bố thông tin nào thuộc Tiêu chuẩn theo Chủ đề này về các tác động của tổ chức liên quan đến quyền riêng tư của khách hàng (Công bố thông tin 418-1).

Xem **Các yêu cầu 4 và 5 trong GRI 1: Tiêu chuẩn cơ sở 2021**.

Có thể đưa ra lý do để lược bỏ những công bố thông tin này.

Nếu không thể tuân thủ việc công bố thông tin hoặc yêu cầu trong việc công bố thông tin (ví dụ: vì thông tin cần công bố là thông tin bảo mật hoặc bị pháp luật cấm), tổ chức phải nêu rõ mục công bố thông tin hoặc yêu cầu mà tổ chức không thể tuân thủ và đưa ra lý do lược bỏ kèm theo lời giải thích trong chỉ mục nội dung GRI. Xem phần **Yêu cầu 6 trong GRI 1: Tiêu chuẩn cơ sở 2021** để biết thêm thông tin về lý do lược bỏ.

Nếu không thể báo cáo thông tin bắt buộc về một mục được chỉ định trong công bố thông tin vì mục đó (ví dụ: ủy ban, chính sách, thông lệ, quy trình) không tồn tại, tổ chức có thể tuân thủ yêu cầu bằng cách báo cáo tình huống thực tế đó.

Tổ chức có thể giải thích lý do không có mục này hoặc trình bày bất kỳ kế hoạch nào để phát triển mục này. Việc công bố thông tin không yêu cầu tổ chức phải thực hiện mục đó (ví dụ: xây dựng chính sách) nhưng phải báo cáo mục đó không tồn tại.

Nếu có ý định công bố báo cáo phát triển bền vững độc lập, tổ chức không cần lặp lại thông tin đã công bố ở nơi khác, chẳng hạn như trên các trang web hoặc trong báo cáo thường niên. Trong trường hợp đó, tổ chức có thể báo cáo nội dung công bố thông tin bắt buộc bằng cách cung cấp tham chiếu trong chỉ mục nội dung GRI đến nơi có thể tìm thấy thông tin này (ví dụ: bằng cách cung cấp liên kết đến trang web hoặc trích dẫn trang trong báo cáo thường niên nơi thông tin đã được công bố).

Các yêu cầu, hướng dẫn và các thuật ngữ được định nghĩa

Những nội dung sau đây được áp dụng trong toàn bộ Tiêu chuẩn này:

Các yêu cầu bắt buộc được trình bày bằng phông **chữ in đậm** và được biểu thị bằng từ “cần phải”. Tổ chức phải tuân thủ các yêu cầu báo cáo theo Bộ Tiêu chuẩn GRI.

Yêu cầu bắt buộc có thể kèm theo hướng dẫn.

Hướng dẫn bao gồm thông tin bối cảnh, giải thích và ví dụ để giúp tổ chức hiểu rõ hơn về các yêu cầu.

Tổ chức không bắt buộc phải tuân thủ hướng dẫn. Tiêu chuẩn cũng có thể bao gồm các khuyến nghị. Đây là những tình huống trong đó một hành động cụ thể được khuyến khích nhưng không bắt buộc phải thực hiện.

Từ “nên” biểu thị khuyến nghị, còn từ “có thể” biểu thị khả năng hoặc lựa chọn.

Các thuật ngữ được định nghĩa sẽ được gạch chân trong văn bản Bộ tiêu chuẩn GRI và được liên kết với định nghĩa tương ứng trong [Bảng thuật ngữ](#). Tổ chức phải áp dụng những định nghĩa trong Bảng thuật ngữ.

1. Công bố thông tin quản lý chủ đề

Tổ chức báo cáo theo Bộ Tiêu chuẩn GRI yêu cầu phải báo cáo cách thức quản lý từng chủ đề trọng yếu của tổ chức đó.

Tổ chức xác định quyền riêng tư của khách hàng là chủ đề trọng yếu yêu cầu phải báo cáo cách thức quản lý chủ đề này theo Công bố thông tin 3-3 trong GRI 3: Chủ đề Trọng yếu 2021 (xem điều khoản 1.1 trong phần này).

Do đó, phần này được thiết kế để bổ sung – nhưng không thay thế – Công bố thông tin 3-3 trong *GRI 3*.

YÊU CẦU

1.1

Tổ chức báo cáo cần phải báo cáo cách thức quản lý theo quyền riêng tư của khách hàng theo Công bố thông tin 3-3 trong GRI 3: Chủ đề Trọng yếu 2021.

2. Công bố thông tin theo chủ đề

Công bố thông tin 418-1 Khiếu nại có căn cứ liên quan đến vi phạm quyền riêng tư của khách hàng và mất dữ liệu khách hàng

YÊU CẦU

Tổ chức báo cáo cần phải cung cấp những thông tin sau đây:

a. Tổng số vụ khiếu nại có căn cứ nhận được liên quan đến vi phạm quyền riêng tư của khách hàng, được phân loại theo:

- i. khiếu nại được nhận từ bên ngoài tổ chức và được tổ chức chứng minh;
- ii. khiếu nại từ các cơ quan quản lý.

b. Tổng số vụ việc rò rỉ, đánh cắp hoặc mất dữ liệu khách hàng.

c. Nếu tổ chức chưa xác định được bất kỳ khiếu nại có căn cứ nào, thì chỉ cần báo cáo tóm tắt về thực tế này là đủ.

Các yêu cầu khi biên soạn

2.1 Khi biên soạn thông tin nêu trong Công bố thông tin 418-1, tổ chức báo cáo cần phải nêu rõ nếu một số lượng đáng kể trong số các vụ vi phạm này liên quan đến những sự kiện từ các năm trước đó.

HƯỚNG DẪN

Bối cảnh

Bảo vệ quyền riêng tư của khách hàng là mục tiêu thường được công nhận trong các quy định của quốc gia và các chính sách của tổ chức. Như được nêu trong *Hướng dẫn của OECD cho các Doanh nghiệp Đa quốc gia* của Tổ chức Hợp tác và Phát triển Kinh tế (OECD), các tổ chức được kỳ vọng sẽ “tôn trọng quyền bảo mật thông tin của người tiêu dùng và thực hiện các biện pháp hợp lý để đảm bảo sự an toàn của dữ liệu cá nhân mà họ thu thập, lưu trữ, xử lý hoặc phổ biến”.

Để bảo vệ quyền riêng tư của khách hàng, tổ chức được kỳ vọng sẽ giới hạn việc thu thập dữ liệu cá nhân, thu thập dữ liệu bằng phương thức hợp pháp, đồng thời minh bạch về cách thu thập, sử dụng và bảo mật dữ liệu. Tổ chức cũng được kỳ vọng sẽ không tiết lộ hoặc sử dụng thông tin cá nhân của khách hàng cho bất kỳ mục đích nào khác ngoài những mục đích đã thỏa thuận, và thông báo trực tiếp cho khách hàng về mọi thay đổi trong các biện pháp hoặc chính sách bảo vệ dữ liệu. Công bố thông tin này đưa ra đánh giá về thành công của các quy trình và hệ thống quản lý liên quan đến việc bảo vệ quyền riêng tư của khách hàng.

Thuật ngữ

Bảng thuật ngữ này trình bày định nghĩa của các thuật ngữ được sử dụng trong Tiêu chuẩn này. Tổ chức phải áp dụng những định nghĩa này khi sử dụng Bộ Tiêu chuẩn GRI.

Các định nghĩa trong danh mục thuật ngữ này có thể chứa các thuật ngữ được định nghĩa chi tiết hơn trong [Bảng Thuật ngữ đầy đủ của Bộ Tiêu chuẩn GRI](#). Tất cả các thuật ngữ có định nghĩa đều được gạch chân. Trường hợp một thuật ngữ chưa được định nghĩa trong Bảng Thuật ngữ này hoặc trong [Bảng Thuật ngữ đầy đủ của Bộ Tiêu chuẩn GRI](#), các định nghĩa được sử dụng và hiểu phổ biến sẽ được áp dụng.

C	chủ đề trọng yếu (material topics) các chủ đề phản ánh những <u>tác động</u> đáng kể nhất của tổ chức đến kinh tế, môi trường và con người, bao gồm cả các tác động đến <u>quyền con người</u> của họ Lưu ý: Hãy xem mục 2.2 trong GRI 1: Tiêu chuẩn cơ sở 2021 và phần 1 in GRI 3: Chủ đề Trọng yếu 2021 để biết thêm thông tin về “chủ đề trọng yếu”.
K	kiếu nại có căn cứ (substantiated complaint) tuyên bố bằng văn bản của cơ quan quản lý hoặc cơ quan chính thức tương tự gửi cho tổ chức theo đó xác định việc vi phạm quyền riêng tư của khách hàng hoặc đơn khiếu nại nộp cho tổ chức mà đã được tổ chức thừa nhận là hợp lý
Q	quyền con người (human rights) các quyền vốn có của tất cả con người, trong đó tối thiểu bao gồm các quyền được nêu trong <i>Tuyên ngôn Quốc tế về Quyền Con người của Liên hợp quốc (UN)</i> và các nguyên tắc liên quan đến các quyền cơ bản được nêu trong Tuyên bố về các Nguyên tắc và Quyền Cơ bản tại Nơi làm việc của Tổ chức Lao động Quốc tế (ILO) Nguồn: Liên hợp quốc (UN), <i>Nguyên tắc Hướng dẫn về Kinh doanh và Quyền Con người: Thực hiện Khung “Bảo vệ, Tôn trọng và Khắc phục” của Liên hợp quốc</i>, 2011; đã sửa đổi Lưu ý: Xem Hướng dẫn 2-23-b-i trong GRI 2: Công bố Chung 2021 để biết thêm thông tin về “quyền con người”. quyền riêng tư của khách hàng (customer privacy) quyền của khách hàng đối với sự riêng tư và không gian cá nhân Ví dụ: nghĩa vụ tuân thủ tính bảo mật; bảo vệ dữ liệu; bảo vệ thông tin hoặc dữ liệu khỏi bị đánh cắp hoặc sử dụng sai mục đích; chỉ sử dụng thông tin hoặc dữ liệu cho mục đích dự định ban đầu, trừ khi có thỏa thuận cụ thể khác Lưu ý: “Khách hàng” được hiểu bao gồm cả người tiêu dùng cuối cùng (người tiêu dùng) và khách hàng doanh nghiệp.
T	tác động (impact) ảnh hưởng đã có hoặc có thể có của một tổ chức đối với kinh tế, môi trường và con người, bao gồm cả <u>nhân quyền</u> của họ; các tác động này phản ánh mức độ đóng góp (tích cực hoặc tiêu cực) của tổ chức đối với <u>phát triển bền vững</u> Lưu ý 1: Tác động có thể là tác động đã xảy ra hoặc có thể xảy ra, tích cực hoặc tiêu cực, ngắn hạn hoặc dài hạn, có chủ định hoặc không chủ định và có thể đảo ngược hoặc không thể đảo ngược. Lưu ý 2: Hãy xem mục 2.1 trong GRI 1: Tiêu chuẩn cơ sở 2021 để biết thêm thông tin về “tác động”.
V	vi phạm quyền riêng tư của khách hàng (breach of customer privacy) không tuân thủ các quy định pháp luật hiện hành và các tiêu chuẩn (tự nguyện) về bảo vệ quyền riêng tư của khách hàng

T**tác động (impact)**

ảnh hưởng đã có hoặc có thể có của một tổ chức đối với kinh tế, môi trường và con người, bao gồm cả nhân quyền của họ; các tác động này phản ánh mức độ đóng góp (tích cực hoặc tiêu cực) của tổ chức đối với phát triển bền vững

Lưu ý 1: Tác động có thể là tác động đã xảy ra hoặc có thể xảy ra, tích cực hoặc tiêu cực, ngắn hạn hoặc dài hạn, có chủ định hoặc không chủ định và có thể đảo ngược hoặc không thể đảo ngược.

Lưu ý 2: Hãy xem [mục 2.1 trong GRI 1: Tiêu chuẩn cơ sở 2021](#) để biết thêm thông tin về “tác động”.

Tài liệu tham khảo

Phần này liệt kê các văn kiện liên chính phủ có giá trị tham chiếu cao được sử dụng trong quá trình xây dựng Tiêu chuẩn này.

Các văn kiện có giá trị tham chiếu cao:

1. Tổ chức Hợp tác và Phát triển Kinh tế (OECD), *Hướng dẫn của OECD cho các Doanh nghiệp Đa quốc gia*, năm 2011.



PO Box 10039
1001 EA Amsterdam
The Netherlands

www.globalreporting.org